Discrete Applied Mathematics 15 (1986) 111-116
North-Holland

NOTE

ITERATIVE CHARACTERIZATIONS OF BOOLEAN ALGEBRAS

Dan SIMOVICI and Corina REISCHER*

Department of Mathematics and Computer Science, University of Massachusetts at Boston, Harbor Campus, Boston, MA 02125, USA

Received 7 June 1985
Revised 31 October 1985

We provide two characterizations of bounded lattices which can be embedded into Boolean algebras based on the iterative properties of algebraic functions over lattices. Such properties are significant from a technical point of view, being related to the synthesis of cascades of switching elements ([2], [3]).

1. Introduction

In his paper [5], D. Schweigert presents a characterization of the class of distributive lattices within the class of lattices using iteration properties of algebraic functions.

The purpose of this Note is to give characterizations of bounded lattices which can be embedded into Boolean algebras using iterative properties of algebraic functions of these lattices.

Let S be a set and assume that $f: S \to S$ is a function. We shall define inductively the iteration powers of f by $f^1(x) = f(x)$ and $f^{n+1}(x) = f(f^n(x))$ for all $x \in S$ and $n \geq 1$.

Let $\mathscr{L} = (L, \{+, \cdot\})$ be a lattice. Schweigert's result asserts that $\mathscr{L}$ is distributive if and only if $f^2 = f$ for every algebraic function of $\mathscr{L}$. The technique of his proof is to show that $\mathscr{L}$ may not contain, under this assumption, any sublattice isomorphic to one of the two lattices whose diagrams are given in Figs. 1(a) and 1(b).

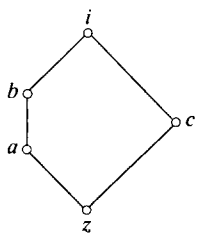

Fig. 1(a).

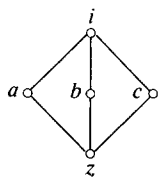

Fig. 1(b).

* On leave from Departement de Mathematiques et d'Informatique, Universite du Quebes a Trois-Rivieres, C.P. 500, Trois-Rivieres, Quebec, G9A, 5H7, Canada.

On another hand, it is known since Schröder [6] that in a Boolean algebra $\mathscr{B} = (B, \{+, \cdot, -, 0, 1\}$ we have $f^3 = f$ for any algebraic function (which is, of course, a weaker iterative property than $f^2 = f$). This result was retrieved by Lyngholm and Yourgrau in [1] and it was used by us in [2] and extended to Post algebras in [3]. We shall prove that his property is a characteristic of Boolean algebras.

Our second characterization of Boolean algebras involves a property of the second iteration of Boolean functions which was discussed by us in [2], in connection with the existence of iterative square roots of Boolean functions.

2. A characteristic iteration property of Boolean functions

Let $\mathscr{B} = (B, \{+, \cdot, -, 0, 1\}$ be a Boolean algebra.

Proposition 1. ([6], [1], [2]). *If $f: B \to B$ is a Boolean function, then $f^3 = f$.*

Proof. Indeed, every Boolean function f (that is, every algebraic function over a Boolean algebra) can be written as

$$f(x) = a\,x + b\,\bar{x},$$

where $a = f(1)$ and $b = f(0)$. It is easy to see that $f^2(1) = f(a) = a + b\bar{a} = a + b$ and $f^2(0) = f(b) = ab$, which gives

$$f^2(x) = (f(0) + f(1))\,x + f(0)\,f(1) \tag{1}$$

Now, we can compute the third iteration by writing

$$f^3(1) = f^2(f(1)) = f(1) + f(0)\,f(1) = f(1)$$

and

$$f^3(0) = f^2(f(0)) = f(0) + f(0)\,f(1) = f(0),$$

which shows that $f^3 = f$.

Theorem 2. *Let $\mathscr{L} = (L, \{+, \cdot, 0, 1\})$ be a bounded lattice having 0 as its first element and 1 as its last element. $\mathscr{L}$ can be embedded in a Boolean algebra if and only if there is a dual automorphism $h: L \to L$ such that in the algebra $\mathscr{B}(L) = (L, \{+, \cdot, h, 0, 1\})$ we have $f^3 = f$, for every algebraic function f.*

Proof. In view of Proposition 1 the conditions of the Theorem are necessary; we choose h as the complement operation.

Conversely, suppose that $\mathscr{L}$ is a lattice such that every algebraic function of the algebra $\mathscr{B}(L)$ satisfies the identity $f^3 = f$.

It is interesting to remark that this weaker property implies the distributivity of $\mathscr{B}(L)$ just as Schweigert's condition does. We follow his approach in proving the

distributivity of $\mathscr{B}(L)$.

Suppose that $\mathscr{B}(L)$ is not distributive. In this case, $\mathscr{B}(L)$ has to contain a sublattice isomorphic to one of the lattices given in Figs. 1(a) and 1(b).

For the first case consider the algebraic function $f(x)=(x+c)b+a$. It is easy to see that $f(z)=a$, $f(a)=b$, $f(b)=b$, that is, $f^3(z)=b\neq f(z)=a$.

For the second case, let g be the algebraic function $g(x)=(x+a)b+c$. For g we have $g(z)=c$, $g(c)=i$ and $g(i)=i$ giving $g^3(z)=i\neq g(z)=c$.

Thus, $\mathscr{B}(L)$ may not contain a sublattice isomorphic to any of the above sublattices, which implies its distributivity.

We have to prove now that the identity $f^3=f$ implies that h has the role of the complement in $\mathscr{B}(L)$. To this end let us remark that $h^3(x)=h(x)$ for $x\in L$ implies $h^2(x)=x$ because h is a bijection. This shows that h is involutive.

Consider the algebraic function w, where $w(x)=(x+a)h(x)$. Due to the involutive property of h we have $h(w(x))=h(x)h(a)+x$.

Applying elementary transformations we obtain

$$w(w(x))=a\,x+x\,h(x)+a\,h(a)\,h(x)$$

and

$$w(w(w(x)))=x\,h(x)+a\,h(x)+ax\,h(a)$$

and, because, $w^3=w$ this implies

$$ax\,h(a)\leq x\,h(x)+a\,h(x).$$

Since h is a dual automorphism of we have $h(0)=1$ and $h(1)=0$. Choosing $x=1$ in the above inequality we obtain $a\,h(a)\leq 0$ which gives, $a\,h(a)=0$. By duality, we have $a+h(a)=1$, which shows that h plays indeed the role of complement in $\mathscr{B}(L)$.

3. Bounded functions and iterations

Let $\mathscr{B}=(B,\{+,\cdot,-,0,1\})$ be a Boolean algebra. A function $f:B\to B$ is *non-constant* if $f(x_1)\neq f(x_2)$ for some $x_1,x_2\in B$.

Proposition 3. *A Boolean function $f:B\to B$ is non-constant if and only if $f(0)\neq f(1)$.*

Proof. The condition is obviously sufficient. Let f be a non-constant Boolean function and assume that $f(0)=f(1)$. Since $f(x)=xf(1)+\bar{x}f(0)$ we have $f(x)=xf(0)+\bar{x}f(1)=(x+\bar{x})f(0)=f(0)$ for $x\in B$, which implies that f is constant. This contradiction shows that $f(0)\neq f(1)$.

Proposition 4. *A Boolean function is non-constant if and only if the second iteration power is non-constant.*

Proof. If $f: B \to B$ is a Boolean function then, using the fact that $f(x) = xf(1) + \bar{x}f(0)$, we obtain for the second iterative power the formula (1). Suppose that f is non-constant. Using the previous Proposition we have $f(0) \neq f(1)$. If $f^2(0) = f^2(1)$ this implies $f(0)f(1) = f(0) + f(1)$ and this, in turn, gives $f(0) = f(1)$. Therefore, we must have $f^2(0) \neq f^2(1)$, which shows that f^2 is non-constant.

Conversely, assume that f^2 is non-constant, that is, $f^2(0) \neq f^2(1)$. Since $f(0)f(1) \neq f(0) + f(1)$ we must have $f(0) \neq f(1)$ (since otherwise, we would have $f(0)f(1) = f(0) + f(1) = f(0) = f(1)$).

We notice from formula (1) that the second iteration power of a Boolean function has a special, simple aspect. This suggests the introduction of the following class of functions:

Definition 1. An algebraic function $f: L \to L$ of a lattice $(L, \{+, \cdot\})$ is *bounded* if we have $p, q \in L$, $p \geq q$ such that $f(x) = px + q$ for $x \in L$.

Obviously, the second iteration power of any Boolean function is bounded.

The referee of this paper has conjectured that this property of Boolean functions might generate yet another characterization of Boolean algebras within the class of lattices. We intend to show that is indeed the case.

Let $\mathscr{L} = (L, \{+, \cdots, 0, 1\})$ be a lattice having the least element 0 and the greatest element 1 and assume that $h: L \to L$ is a dual morphism of this lattice.

Theorem 5. *The lattice $\mathscr{L}$ can be embedded in a Boolean algebra if and only if the second iterative power of every non-constant algebraic function of the algebra $(L, \{+, \cdot, h, 0, 1\})$ is a non-constant bounded function.*

Proof. The reader will notice that now h is required to be a dual morphism not an automorphism as in Theorem 2. The condition is clearly necessary in view of the equality (1) and Proposition 4.

Let us prove that the condition is sufficient. We will show that $(L, \{+, \cdot, 0, 1\})$ is a distributive lattice and h plays the role of the complement.

Suppose that L would contain a sublattice isomorphic to the lattice from Fig. 1(a). The function $f: L \to L$ given by $f(x) = (x + c)b + a$ is non-constant since $f(z) = a$ and $f(a) = b$. Therefore its second iterative power must be a bounded non-constant function which gives

$$[(x + c)b + a + c]b + a = \alpha x + \beta,$$

for $x \in L$ and $\alpha, \beta \in L$ with $\alpha \geq \beta$.

Choosing $x = 0$ in the above equality gives $\beta = (a + c)b + a$, which, in turn, gives $\beta = b$ (see (Fig. 1(a)). Taking $x = 1$ in (2) gives $b = \alpha + b$, hence $\alpha \leq b$; since $\alpha \geq \beta = b$, we have $\alpha = \beta = b$ and this implies that the second iteration power of f is the function $k: L \to L$, where $k(x) = bx + b = b$, which is a constant. Therefore, it is impossible for

L to contain a sublattice isomorphic to the one from Fig. 1(a).

Suppose now that L would contain a sublattice isomorphic to the lattice from Fig. 1(b). The function $g: L \to L$ given by $g(x) = (x+a)b + c$ is non-constant since $g(z) = c$ and $g(c) = i$; its second iteration should have the form

$$[(x+a)b + c + a]b + c = \gamma x + \delta,$$

for some $\gamma, d \in L$, $\gamma \geq \delta$.

Again, choosing $x = 0$ we get $b + c = \delta$, which gives $\delta = i$ (see Fig. 1(b)). Choosing $x = 1$ we have $b + c = \gamma + \delta$, hence $i = \gamma + i$. This implies $\gamma \leq i$ and, since $\gamma \geq \delta = i$, we have $\gamma = \delta = i$. Therefore, the second iteration power of g is the function $l: L \to L$, where $l(x) = ix + i = 1$ for $x \in L$, which is a constant function. This contradiction shows that L may not contain a sublattice isomorphic to the lattice from Fig. 1(b). We conclude that $(L, \{+, \cdot, 0, 1\})$ is a distributive lattice.

Since $h^2(x) = \lambda x + \mu$ for some $\lambda, \mu \in L$ and $\lambda \geq \mu$, we have $h^2(0) = 0 = \mu$ and $h^2(1) = 1 = \lambda + \mu$, which implies $\lambda = 1$ and $\mu = 0$. Therefore, $h^2(x) = x$, which shows that h is involutive.

Consider now the function $u: L \to L$ defined by $u(x) = x\,h(x)$. We will prove that u is a constant function. Suppose that u is non-constant. In this case, its second iteration power should be also a bounded non-constant function.

We have $u^2(x) = x\,h(x)\,h[x\,h(x)] = x\,h(x)(h(x) + x) = x\,h(x) = \sigma x + \tau$ for $\sigma, \tau \in L$, $\sigma \geq \tau$.

Taking $x = 0$ we obtain $\tau = 0$ and taking $x = 1$ we have $0 = \sigma + \tau$, which implies that the second iteration power of u is the function $v: L \to L$ given by $v(x) = \sigma x + \tau = 0\,x + 0 = 0$, which is a constant function. Therefore, u must be a constant function. Because $u(0) = 0$, we have $u(x) = 0$ for $x \in L$, hence $x\,h(x) = 0$; by duality, we have $x + h(x) = 1$ for all $x \in L$, which shows that h plays the role of the complement.

Acknowledgements

The authors gratefully acknowledge the suggestions of the referee.

This research has been supported by the grant A4063 from the Natural Science and Engineering Research Council (NSERC) of Canada.

References

[1] C. Lyngholm and W. Yourgrau, A double-iterative property of Boolean functions, Notre Dame J. Formal Logic 1 (1960) 111–114.

[2] C. Reischer and D.A. Simovici, Associative algebraic structures in the set of Boolean functions and some applications in automata theory, IEEE Trans. Computers 20 (1971) 298–303.

[3] C. Reischer and D.A. Simovici, Several remarks on iteration properties of switching functions, Proc. 12th International Symposium on Multiple-Valued Logic, Paris, France (1982) 244–247.

[4] S. Rudeanu, Boolean Functions and Equations (North-Holland, Amsterdam; American Elsevier, New York, 1974).

[5] D. Schweigert, Ueber idempotente Polynomfunktionen auf Verbandes, Elemente des Mathematik 30(2) (1975) 30–32.

[6] E. Schröder, Vorlesungen über die Algebra der Logik, 3rd volume (Leipzig 1895; reprinted by Chelsea, New York, 1966).